EXAMINATION PLANNING CHAPTER 3

(FILE NAME ON DISK # 1 = S1C3.WPD)

The IS regulatory program supports the overall goal of financial institution and servicer regulatory reviews. The reviews are designated to identify and correct information on technology-related risk exposures of significance that threaten the financial institutions industry. The information is updated regularly to encourage uniformity among FFIEC member agencies in regulating financial institutions and their service bureau vendors. A properly directed and managed IS regulatory program may be achieved by:

- Supervising IS program performance, including program development, quality control, and staff development.
- Maintaining a risk-based IS program for allocation of limited IS examination resources.
- Scheduling IS examinations.
- Supervising work to ensure alignment with safety and soundness objectives.
- Supervising work completeness, accuracy, and conformance with regulatory policies and procedures.
- Distributing IS reports of examination of institutions and service bureaus.
- Reviewing written response to report findings.

IS EXAMINATION TYPES

IS examiners are responsible for examining service bureaus, in-house data centers, and other high risk situations (e.g., systems conversions in serviced institutions). The types of IS examination activities performed by FFIEC IS examination departments are as follows.

Institution Operations

- *In-house* – Institution that operates its own data center and does not service others (if other institutions are serviced, the institution should be treated as a local or regional service bureau).
- *Serviced* – Institutions serviced primarily by service bureaus.
- *Interagency Shared Application Software Reviews (SASR)* – Interagency reviews of widely used turnkey software products. SASR reports are distributed by agencies for internal use only.

Service Bureau Operations

- *MDPS* – Multiregional data processing servicers that may be regional or national in scope and that service more than one class of financial institutions.
- *National* – Service bureaus that are not part of the MDPS program and that service financial institutions on a national scale.
- *Regional* – Service bureaus that service financial institutions on a less than national scale but that have locations in a sufficient number of contiguous states to be considered regional in scope.
- *Local* – Service bureaus that service one or more institutions in the same region.

FREQUENCY OF IS EXAMINATIONS

The frequency of in-house and service bureau examinations is based on the concept of risk based supervision/regulation, i.e., the lower the risk, the less the regulatory scrutiny. FFIEC member agencies direct resources to those data centers or situations that need greater supervisory attention. The lower the rating, (4 or 5), the more closely the data center is monitored and more frequently examined. Data centers assigned higher and better ratings, (1 or 2), generally require less regulatory scrutiny. Other factors that might prompt more frequent examinations include a deteriorating condition, enforcement action, substantial plans for IS replacement, or a change of control. The frequency of

in-house institution examinations is determined by the policy of each FFIEC member agency.

Service Bureaus

Service bureau examinations which generally are not linked to a safety and soundness examination of a financial institution are scheduled under separate criteria. In all cases the IS examinations of regional and local service bureaus must be coordinated with other regulatory agencies. Service bureaus in the national Multiregional Data Processing Servicer (MDPS) Program are examined on an interagency basis and administered and coordinated through the Washington office of each agency.

The examination schedule for service bureaus should consider the risk level of serviced institutions as discussed under the supervision by risk concept (see Chapter 2 for additional information.)

Serviced Institutions

IS-related risks in institutions' serviced primarily by service bureaus are examined by safety and soundness examiners using appropriate procedures. These examinations are normally part of the regularly scheduled safety and soundness examination.

Shared Application Software Reviews

Interagency Shared Application Software Reviews (SASR) of vendor turnkey software products will be performed periodically (generally one per quarter) as determined by the FFIEC IS Subcommittee. SASR reviews document the characteristics of the software products to assist examiners in examining institutions using the vendor products. There are no ratings for these reviews. Districts/regions, at their discretion, may perform software reviews on selected turnkey software products that are used widely by institutions in their region.

TIME STANDARDS FOR IS EXAMINATIONS

The intent is for IS examinations of in-house institution data centers to be conducted concurrently with those for the safety and soundness supervisory efforts in a financial institution. IS examinations of service bureaus should be performed for both MDPS and non-MDPS jointly with other supervisory agencies. Each agency has developed procedures and guidelines for scheduling and conducting IS examinations to allocate IS examination specialists properly. These scheduling procedures should be adjusted and the institution notified when the IS examination cannot be performed concurrently with the safety and soundness examination,.

Time allocated for an on-site IS examination is based on the risk and complexity of the examination. After arrival on-site the IS EIC should validate the scope and risk assumptions to ensure time planned is adequate to address the identified risks. If additional on-site examination resources are required the IS EIC, must consult with the safety and soundness EIC on concurrent examinations and/or with the IS examination manager to evaluate the request for more resources. If approved, the IS EIC must reevaluate and modify the examination scope to schedule the use of any additional resources.

Shared Application Software Review (SASR)

One examiner from each agency is normally assigned for two weeks to each SASR review. The lead agency's EIC may work for up to three additional weeks to finalize the SASR report. The additional time commitment depends on the complexity of the product, scope of prior planning, and extent of vendor support received.

FINANCIAL INSTITUTION EXAMINATIONS

IS examinations of in-house institution data centers should be conducted concurrently with safety and soundness examinations according to member agency policy. Safety and soundness and IS examiners should work together as a team. The safety and soundness EIC may include statements on the IS examination findings in the safety and soundness report.

Each agency's organizational structure, position titles, and responsibilities vary. Guidelines for conducting concurrent IS examinations are developed by each agency. The procedures should be adjusted accordingly when the IS examination cannot be performed at the same time as the safety and soundness examination.

The relationship between the safety and soundness EIC and the IS EIC is similar for all agencies. Although

agency organizational structures, IS related job descriptions, and reporting lines differ, they ascribe essentially the same duties to the IS examiner.

IS Examiner-in-Charge Responsibilities

The IS EIC is responsible for the administration and overall performance of the IS examination. These responsibilities include, but are not limited, to:

- Performing sufficient planning to identify and evaluate IS risk areas and ensuring that the scope of IS examination covers high risk activities. Reviewing internal and external audits to supplement the examination process.

- Preparing IS examination objectives and procedures for activities included in the scope.

- Preparing a project plan containing scope, objectives, procedures and often a budget; the examiner allocation should reflect a breakdown of total hours and a schedule for significant scope activities.

- Prior to the start and during concurrent examinations, discussing and resolving scoping and resource and administrative issues with the safety and soundness EIC.

- Keeping the safety and soundness EIC and IS examination manager informed of scheduled meetings with management and attending meetings.

- Ensuring that the examination procedures are completed in accordance with the appropriate sections of the *1996 FFIEC IS Examination Handbook* and with the approved project plan.

- Communicating examination findings to the IS examination manager and safety and soundness EIC.

- Holding exit meetings with IS management to review findings of the examination and recommendations for follow-up.

- Preparing a "camera ready" ROE with an assigned rating and clear, concise summary of findings. The ROE should reference the objectives of the scoping document and workprogram and be supported by workpapers.

- Signing IS ROE. The ROE must be signed by an accredited IS examiner.

- Forwarding the IS ROE to the IS examination manager for review; incorporating review comments as appropriate, and forwarding "camera ready" IS ROE to the safety and soundness EIC.

- Conducts the IS portion of safety and soundness board of directors meetings for 4- and 5-rated institutions. The IS examination manager should participate in these meetings as appropriate.

- Reviewing and evaluating IS examiners.

Supporting IS Examiner Responsibilities

- Performing assigned workprogram sections per FFIEC examination guidelines.

- Documenting findings in workpapers and finding sheets.

- Identifying deficiencies and communicating significant findings to the EIC and other examiners.

- Discussing findings with management.

- Ensuring that workpapers are cross-referenced properly to document, and support substantial findings and conclusions.

- Preparing findings and recommendations in "camera ready" report format.

Safety and soundness Examiner-in-Charge – responsibilities of the safety and soundness EIC include:

- Working closely with the IS EIC on planning and performance of concurrent examinations, scheduling of management meetings, and resolving related IS examination issues.

- Attending opening and closing meetings and other meetings at which significant IS issues are discussed, when concurrent examinations are conducted.

- Reviewing IS ROE and considering IS examination findings to determine the adequacy of the institution's system of internal controls and safety and soundness ratings.

- Incorporating significant IS findings in the safety and soundness ROE, as appropriate, and attaching the OPEN section of the IS ROE as an addendum to the safety and soundness ROE.

- Conducting board of directors meetings.

- Modifying regulatory plan, as necessary.

IS Examination Manager – The IS examination manager's responsibilities include:

- Ensuring that district/regional IS examining resources are used effectively based on risk profile of supervised institutions.

- Coordinating requests for financial institution, service bureaus, and MDPS IS examinations from agency management. Monitoring revisions to IS examination schedule and adjusting as necessary.

- Assigning an IS EIC and supporting examiners.

- Reviewing and signing or recommending for signature the final IS ROE for the district/region.

- Supervising the performance of IS examinations and high risk situations (e.g., system conversions). Coordinating MDPS examination activities with Washington headquarters and the MDPS EIC.

- Ensuring the overall quality, competency and consistency of IS examinations, and compliance with national and FFIEC standards.

- Conducting meetings with management and boards of directors.

- Reviewing service bureau ROE's and collaborating with agency/interagency management for distribution to the service bureaus, IS client serviced institutions, and to other regulatory agencies.

- Reviewing management responses to findings in ROE.

SERVICE PROVIDERS' EXAMINATIONS

Agency management must ensure that all service bureaus within its area of responsibility receive IS examinations as required member agency and FFIEC policy. Most, if not all, of the activities and responsibilities of the IS EIC, supporting IS examiners and to a lesser extent the IS manager are the same in a service provider examination.

IS Examiner-in-Charge Responsibilities

In a servicer examination the IS EIC is responsible for:

- Communicating examination findings to the IS examination manager and EIC for interregional or interagency service bureau examinations.

- Holding exit meetings with service bureau management to review examination findings and recommendations for follow-up.

- Forwarding ROE to IS examination manager for review. Incorporating review comments and providing final copy to IS examination manager.

- Conducting IS board of directors meeting for service bureaus.

- Reviewing and evaluating IS examiners.

- Assisting in scheduling interagency examinations.

- Reviewing scope documents for MDPS examinations.

IS Examination Manager – The IS examination manager's responsibilities include:

- Preparing the transmittal letter for the servicer's board of directors.

- Reviewing MDPS ROE's.

- Sending MDPS ROE's to service bureaus and districts/regions.

MDPS Examiner-in-Charge

In addition to the duties previously described in the Examiner-in-Charge Responsibilities section the MDPS

EIC will be responsible for:

- Scheduling and setting the scopes of MDPS examination of corporate headquarters and remote data centers, based on input from all effected agencies.
- Coordinating resources to conduct examinations under guidance from Washington headquarters.
- Reviewing individual MDPS data center ROE's and resolving examination issues with other agency personnel.
- Preparing MDPS ROE, assigning rating and signing the ROE.
- Sending ROE to Washington headquarters for final review. Distribution occurs from the agency headquarter's office or the district or region, as appropriate.
- Reviewing service bureau responses to ROE findings and distributing to Washington headquarters.

GATHERING INFORMATION

The IS EIC must gather, organize, and analyze available information prior to beginning an on-site IS examination. Sources of information include, but are not limited, to:

- The IS examination permanent file.
- The supervisory/regulatory plan for the financial institution.
- Prior examination reports, workpapers, and recommendations.
- Supervisory actions and correspondence.
- Internal and external audit reports, when available.
- External databases (NEXIS/LEXIS). Discussions with appropriate regional personnel and other agencies.

SCOPING THE EXAMINATION

Effective examinations must be properly pre planned to ensure that significant IS risks are identified and appropriate regulatory action taken. Once the risk areas have been identified the examination planning scope involves reviewing available information to determine specific examination procedures to be performed and the depth of coverage (e.g., Tier I and Tier II).

The IS EIC must determine the scope of work and estimate the hours required to complete it. The examination of all potential risks should consider staffing, time, and benefits. Adequate time must be allocated to higher risk activities. In service bureau examinations that assess more than one data center, the scope document should include the headquarters location and all subsidiary data centers.

Scoping procedures should emphasize risk areas. Some of the risk areas that should be considered while developing the scope are: IS audit adequacy, management planning/direction, conversion activity(s), application development/maintenance, data/system/physical security, networking, corporate contingency planning activities, and computer system controls.

After the scope of examination is determined, an IS examination scope memorandum is prepared to document the areas to be examined. The scope memorandum should outline the objectives of the examination, assignments, budget, and other relevant information. When examining in-house data centers, the examiner should visit the data center and talk to the IS management. He/she should gather basic information to aid in: identifying high risk areas and known problems, and determining the size and complexity of the data center and software systems. On concurrent examinations, all meetings with IS management should be coordinated with the safety and soundness EIC. On MDPS examinations, all meetings with the servicer senior management should be coordinated with the lead agency MDPS EIC and Washington headquarters.

The initial examination scope is based on preexamination analysis and on-site review of IS data processing and management information systems. It should be refined at the start of, and during, the examination as additional information is obtained and reviewed. Off-site materials that should be considered in determining the scope are listed in the previous section on Gathering Information. The preliminary

scope provides information to determine staff requirements, the examination start date, and strategies for conducting the examination. Upon starting the on-site activity, additional information that may affect the scope should be reviewed as soon as possible.

During the task of setting the scope and throughout an examination, the IS EIC should maintain regular communications with the safety and soundness EIC, IS examination manager, MDPS EIC, and other agencies, as necessary. Anticipated significant changes in scope, projected staffing, and completion dates should be communicated promptly to the appropriate persons. The team should know the regulatory plan objectives and the approach for meeting them. In that regard, the IS EIC must communicate effectively with the safety and soundness EIC and team members.

COORDINATING THE EXAMINATION

IS examinations of institutions with in-house data centers should be conducted concurrently with safety and soundness examinations. In planning and coordinating those IS examinations, the IS EIC works closely with the safety and soundness EIC. The safety and soundness EIC should be kept informed of the status of the IS examination. The examination activities on service bureau examinations, should be coordinated with the IS examination manager and other staff.

When conducting concurrent examinations, the safety and soundness EIC should be advised of the following information at the start of, and during the examination:

- The IS examination start date.
- The time and location of meetings with management.
- The IS examination scope and schedule.
- Interim status and progress reports as required by IS manager.
- Any material findings or modification of examination scope.
- The agenda for the exit conference prior to meeting with management.
- Drafts of the proposed IS ROE and the transmittal letter.

Sometimes, IS examinations of in-house centers may be conducted separately from safety and soundness examinations. The IS EIC should coordinate the IS examination work with the safety and soundness EIC.

Joint Examinations

The IS examiner may participate in joint IS examinations of service bureaus with other districts and federal or state agencies. Those examinations require that the scoping, scheduling, and preparation of the ROE be coordinated with the other agencies. For other joint examinations, IS examiners must be flexible and cooperative when working with other districts/regions and regulatory agencies.

NOTIFICATION OF THE EXAMINATION

For concurrent examinations, the institution will be notified in the safety and soundness request letter that an IS examination will be conducted. When conducting separate IS examinations, the notification letter should be mailed at least four weeks prior to the start of the examination. The letter should be addressed to the Chief Executive Officer (CEO) of the institution or servicer and signed by appropriate regulatory personnel. The letter should be sent to appropriate safety and soundness personnel and key contact people at the institution. For service bureau examinations, a client list may also be requested in the notification letter or in a separate request letter.

For service bureau examinations, the IS EIC or IS examination manager contacts the IS examination contact person prior to starting the examination. The initial communication should inform the service bureau management that an IS examination has been scheduled, the date, requested information, the name of the EIC, and other details.

At least one week prior to the projected start date, the IS EIC should call the institution or servicer to verify that the letter was received, to answer any questions, and to make arrangements for on-site work. The IS examiner will have frequent contact during the examination with the management of both the internal audit department and the data processing department. It is appropriate to meet initially with them and their staff. At the start of the examination this management meeting should be scheduled on-site to discuss:

- New developments since the last audit and/or examination, i.e., changes in control or management.
- Actions taken to correct deficiencies mentioned in prior examination and audit reports.
- Operating performance in comparison with the budget.
- Significant changes in operations or strategies.
- Significant concerns of management.
- Economic and competitive conditions in market area.
- Significant planned or anticipated changes and developments in IS hardware or software.

The introductory or later meetings may also address:

- Time limits for receiving requested information.
- The availability of the examiners to answer questions from the staff preparing requested information.
- Administrative details, such as names of key contact people, facilities and parking, work hours, and use of equipment.
- The duration of the examination, any planned interruptions (these should be kept to a minimum), names of examiners, and methods to ensure the efficient use of examiner's time.
- A meeting with the independent auditor, if applicable.
- Review of independent audit workpapers.
- Timing for regular meetings with the CEO to discuss the progress of the examination and to address any other issues of concern to the CEO or the IS EIC.